




DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT INFORMATION INTEGRITY	POLICY NO. 559.01	EFFECTIVE DATE 04/20/2005	PAGE 1 of 2
APPROVED BY:  Director	SUPERSEDES 500.45 04/20/2005	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To protect Protected Health Information (PHI) and other confidential information from improper alteration and/or destruction.

POLICY

- 2.2 The Department of Mental Health (DMH) must ensure that appropriate authentication mechanisms are utilized to corroborate that stored data within its possession has not been altered or destroyed in an unauthorized manner.
- 2.3 System Managers/Owners are responsible for implementing integrity checks using the above-referenced authentication mechanisms and reporting any suspicious findings to the Departmental Information Security Officer. All Workforce Members must also report any unauthorized data modification or destruction to the System Managers/Owners.

DEFINITION

- 3.1 Integrity Control: The mechanism or procedure that preserves the property that data or information have not been altered or destroyed in an unauthorized manner.
- 3.2 Protected Health Information: Individually identifiable information:
(1) Except as provided in paragraph (2) of this definition, that is:
(i) Transmitted by electronic media;
(ii) Maintained in any medium; or
(iii) Transmitted or maintained in any other form or medium.
- (2) Protected health information excludes individually



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION INTEGRITY	559.01	04/20/2005	2 of 2
APPROVED BY: Director	SUPERSEDES 500.45 04/20/2005	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

identifiable health information in:

- (i) Education records
- (ii) Employment records

- 3.3 System The person who is responsible for the operation and use of
Managers/Owners: a system.

For a more complete definition of terms used in this policy and/or procedure, see the DMH Security Glossary, Attachment I of Policy No. 555.02, Information and Technology Security Policy.

PROCEDURE

- 4.1 Follow the procedures detailed in Attachment I.

AUTHORITY

MANDATED BY 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308
(a)(3)(ii)

ATTACHMENT

Attachment I DMH Information Integrity Procedures

REVIEW DATE

This policy shall be reviewed on or before January 2010.